UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/782,825	02/14/2001	Frank J. DiSanto	Copy-60	1728

7590 10/18/2005	**EXAMINER**
Plevy & Howard	CHAI, LONGBIT
600 North Easton Road	
Willow Grove, PA 19090	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>*7/25/2005*</u>.
2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-10* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) *1-10* is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on <u>*25 June 2001*</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)
1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 11 – 28 have been canceled; claims 1 – 4 have been amended in an amendment filed 7/25/2005.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/4/2005 has been entered.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claim 1 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

The claim limitation of claim 1 "using a received public key and synchronizing indicator in combination with said retained private key to determine, and retain an encryption key" is not enabled by the specification. As understood by the examiner, the sequence to generate a plurality of encryption keys is well defined in the specification (Table 1); however, the exact function to generate each individual encryption key based upon said three parameters disclosed (i.e., public key, private key and synchronizing indicator) is not specifically defined in the specification (Para [0025]). Therefore, one skilled in the art clearly would not know how to make and use the same from the claimed invention to determine, and retain the encryption key as claimed.

Even though Applicant indicated methods of determining encryption keys are well known in the art (Para [0025]), but that is limited to public-and-private key systems and is not disclosed on the encryption key specifically created from a set of public key, private key and synchronizing indicator as recited in claim 1.

Any other claims not addressed are rejected by virtue of their dependency should also be corrected

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.   Claims 1 – 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Gennaro (Patent Number: 6009176), in view of Bjerrum (Patent Number: Re.36310).

5.   As per claim 1, Gennaro teaches a method for facilitating secure communications

among at least two parties over a communication network, comprising:

retaining a first private key and transmitting a corresponding first initial public key

and synchronizing indicator (Gennaro: Column 10 Line 4 – 7: a digital signature on the

purported hash value computed on the first original block can be considered as the

synchronizing indicator and a first private key retained is used for digital signature as

taught by Gennaro);

Gennaro teaches the first private key must be retained during the ciphering

process (Gennaro: Column 7 Line 6 – 25: Gennaro teaches the previous private key SK

$(i – 1)$ needs to be retained in order to decrypt the current data block (i)). However,

Gennaro does not disclose expressly using a received second public key and second

synchronizing indicator in combination with said retained first private key to determine,

and retain a first encryption key.

Bjerrum teaches using a received second public key and second synchronizing

indicator in combination with said retained first private key to determine, and retain a

first encryption key (Bjerrum: Column 18 Line 47 – 62 and Column 37 Line 52 – 56).

It would have been obvious to a person of ordinary skill in the art at the time the

invention was made to combine the teaching of Bjerrum within the system of Gennaro

because (a) Gennaro teaches encryption / decryption of the security sensitive

information based on previously retained encryption / decryption keys and (b) Bjerrum

discloses encryption / decryption of the security sensitive information can be further

based on previously exchanged random number to enhance the security to ensure the

secured communications between any two stations

determining a second private key, a third public key and a third synchronizing

indicator wherein said second private key is retained with said first retained private key

(Gennaro: see for example, Column 10 Line 4 – 7, Column 7 Line 12 – 15 and Column

7 Line 19 – 24: Gennaro teaches the previous private key SK (i – 1) needs to be

retained in order to decrypt the current data block (i));

encrypting at least said third synchronizing indicator using said first encryption

key (Bjerrum: Column 37 Line 9 – 13: encrypting the random number (i.e. synchronizing

indicator) with the first encryption key as taught by Bjerrum).

transmitting said third public key and encrypted third synchronizing indicator

(Gennaro: Column 10 Line 4 – 7: transmitting a public key along with a digital signature

on the purported hash value computed on the data block can be considered as the

synchronizing indicator as taught by Gennaro);

decrypting a received fourth synchronizing indicator using said first encryption

key (Bjerrum: Column 37 Line 9 – 13: decryption is the counter part of the encryption);

determining a second encryption key from said second private key, a fourth

public key and said decrypted fourth synchronizing indicator, wherein said second

encryption key is retained with said first encryption key (Gennaro: see for example,

Column 7 Line 12) & (Bjerrum: see for example, Column 37 Line 52 – 56)..

6.   As per claim 2, Gennaro as modified further teaches determining a next private

key and a next information item set, encrypting at least one element of said next

information item set, transmitting said next encrypted information element, decrypting

said received encrypted information item element; and, determining a next encryption

key from said next private key and said decrypted information item are repeated until a

known number of encryption keys (Bjerrum: Column 18 Line 47 – 62 and Column 37

Line 52 – 56) & (Gennaro: see for example, Column 3 Line 25 – 26, Column 5 Line 44 –

46, Column 7 Line 12 – 15 and Column 7 Line 19 – 24: Gennaro discloses a known

number of encryption keys need to be determined in order to repeat for all the data

blocks in a digital stream which is being divided into a known number of data blocks

because the previous private key SK (i – 1) needs to be retained in order to decrypt the

current data block (i)).

7.   As per claim 3, Gennaro as modified further teaches said information item

element comprises a public key (Bjerrum: see for example, Column 18 Line 59 – 60:

Bjerrum teaches the encryption key can be created based on other person's public key

as well as his own digital signature (i.e. his own private key).

8.   As per claim 4, Gennaro as modified further teaches said information item

element comprises a synchronizing indicator (Bjerrum: see for example, Column 37

Line 52 – 56: Bjerrum teaches encryption key is made by use of a previously exchanged

random number which is qualified as a synchronizing indicator).

9.   As per claim 5, Gennaro as modified further teaches selecting at least one of

said retained encryption keys alternatively (Bjerrum: see for example, Column 22 Line

45 – 47: Bjerrum teaches data encryption keys being used were arranged in a known

sequence (or pre-selected order) beforehand. One of ordinary skill in the art,

furthermore, would have expected choosing the encryption alternatively as one form of

a pre-selected orders can perform equally well with other options because either

selection performs the same function of preventing security bleaching).

10.   As per claim 6, Gennaro as modified further teaches selecting a known

encryption key (Bjerrum: see for example, Column 22 Line 45 – 47: Bjerrum teaches

data encryption keys being used were arranged in a known sequence (or pre-selected

order) beforehand).

11.   As per claim 7, Gennaro as modified further teaches known encryption key is

such that an output value is the same as an input value (It is evident that no encryption

s needed as long as the communication is secured).

12.   As per claim 8, Gennaro as modified further teaches encryption keys are

selected in a known sequence (Bjerrum: see for example, Column 22 Line 45 – 47:

Bjerrum teaches data encryption keys being used were arranged in a known sequence

(or pre-selected order) beforehand).

13.   As per claim 9, Gennaro as modified further teaches known sequence

corresponds to an order of retention of said encryption keys (Bjerrum: see for example,

Column 37 Line 12 – 13 and 22 Line 45 – 47).

14.   As per claim 10, Gennaro Gennaro as modified further teaches known sequence

corresponds to an order pre-selected by said parties (Bjerrum: see for example, Column

22 Line 45 – 47: Bjerrum teaches data encryption keys being used were arranged in a

known sequence (or pre-selected order) beforehand).

        Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Longbit Chai whose telephone number is 571-272-3788.

The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

        If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

Primary Examiner
AU 2131
10/11/05

LBC